Computer Science Department

TECHNICAL REPORT

Set-Theoretic Reductions of Hilbert's Tenth Problem

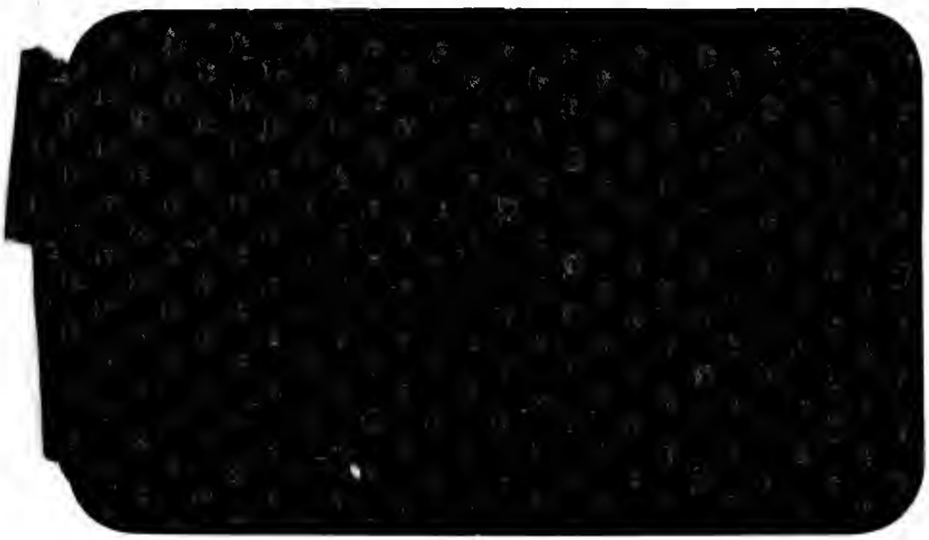
D. Cantone
V. Cutello
A. Policriti

Technical Report 449

May 1989

NEW YORK UNIVERSITY

Department of Computer Science
Courant Institute of Mathematical Sciences
251 MERCER STREET, NEW YORK, N.Y. 10012



Set-Theoretic Reductions of Hilbert's Tenth Problem

D. Cantone
V. Cutello
A. Policriti

Technical Report 449

May 1989

SET-THEORETIC REDUCTIONS OF HILBERT'S TENTH PROBLEM *

D. CANTONE
V. CUTELLO
Computer Science Department
Courant Institute of Mathematical Sciences, New York University
251 Mercer St., 10012 New York, New York; and
Dipartimento di Matematica, Università di Catania
Viale A. Doria 6A, 95125 Catania, Italy.

A. POLICRITI
Computer Science Department
Courant Institute of Mathematical Sciences, New York University
251 Mercer St., 10012 New York, New York; and
Dipartimento di Matematica e Informatica, Università di Udine
Via Zanon 6, 33100 Udine, Italy.

1 Introduction

The size of the elementary deductions that a computerized verifier is able to carry out automatically is directly related to the richness of its *inferential core*, i.e. the collection of routines which allow the verifier to certify the correctness of purported proofs. Thus, in the last decade, as part of a long term project for the design and implementation of a set-theoretic based proof verification system, jointly conducted at New York University, Catania University (Italy), and ENIDATA-Bologna (Italy) (cf. [CS88]), the decision problem for several fragments of set theory has been investigated very actively.

Satisfiability tests (and, dually, validity tests) have been provided for numerous classes of unquantified and quantified formulae of set theory.

The basic language that has been considered is *MLS* (an acronym for Multi-Level Syllogistic), i.e. the unquantified language of set theory with $=$, $\subseteq$, and $\in$ as predicate symbols, $\cup$, $\cap$, and $\setminus$ as function symbols, and the propositional connectives $\wedge$, $\vee$, $\rightarrow$, $\leftrightarrow$, and $\neg$. A decision test for *MLS* has been first given in [FOS80a].

Subsequently, many extensions of *MLS* with various other set operators and predicates have also been shown to have a solvable satisfiability problem. Here we cite:

*This work has been partially supported by ENI and ENIDATA within the AXL project.

- *MLS* extended by *rank* related constructs (see [CFMS87,CCF88,CC88a]);

- *MLS* extended by a choice operator (see [FO87,CFO88,Fer,PP,CFOP88]);

- *MLS* extended by the general union operator (see [CFS87]) and by the powerset operator (see [CFS85,Can]);

- *MLS* extended by map related constructs (see [FOS80b,CS]);

- *MLS* extended by cardinality constructs (see [FOS80a,CC89]).

Also, some quantified classes of set-theoretic formulae properly extending *MLS* have been shown decidable. Specifically, in [BFOS81] a decision procedure has been given for the $(\forall)_0$ *simple prenex* formulae, namely propositional combinations of all purely universal restricted prenex formulae of the form

$$(\forall x_1 \in y_1)\cdots(\forall x_n \in y_n)\psi ,$$

such that no x_i can be a y_j (i.e. quantified variables can not be nested) and where ψ can involve $=$, $\in$ and the predicates

$$\textit{is\_an\_integer}(x) \quad \text{and} \quad \textit{is\_an\_ordinal}(x).$$

Recently, [PP] has considered the case in which nested variables are allowed, provided that the matrix ψ satisfies certain additional conditions.

Other variants of the quantified case have also been studied in [CCF88] and [CC88b], where decision procedures are derived when the operator $rank(x)$ and the predicate $Finite(x)$ are respectively allowed in the matrix ψ.

Finally, in [Gog78] and [Gog79] it is shown the completeness of two classes of sentences of set theory.

In view of this vast body of results, the problem to set "upper bounds" to the decidable is then of the utmost importance for understanding how much of set theory one can hope to mechanize.

This problem has been recently investigated in [PP88], where it is shown that Gödel's first incompleteness theorem can be proved in a surprisingly weak theory of sets with formulae of very low complexity. As a consequence, it is shown that the satisfiability problem for propositional combinations of restricted prenex formulae with two quantifiers alternations (the so-called $(\forall\exists\forall)_0$-formulae) is unsolvable.

In this paper, we strengthen the preceding undecidability result with respect to the complexity of the formulae only, the underlying theory being essentially the standard Zermelo-Fraenkel set theory. In particular, we will show that just one quantifier alternation suffices to obtain undecidability. This class of formulae will be denoted by $(\forall\exists)_0$.

In particular, we will show how to effectively associate a suitable $(\forall\exists)_0$-formula φ to any given polynomial Diophantine equation D in such a way that φ is satisfiable by a set model if and only if D has integer solutions. Then, the undecidability of the $(\forall\exists)_0$-formulae will follow directly from the unsolvability of Hilbert's tenth problem, i.e. the problem to decide for a polynomial

Diophantine equation whether or not it has integer solutions (cf. [Mat70]; see also [Dav73] and [DMR76] for beautiful expository accounts on Hilbert's tenth problem).

As by-products, the undecidability of other classes of quantified and unquantified formulae will be also derived.

If the class of $(\forall)_0$-formulae is decidable (as we conjecture) then our result allows to locate precisely the boundary between the decidable and the undecidable in set theory.

In the following section, we will give some basic definitions; then in Section 3 we will prove the undecidability of two variants of the unquantified theory *MLS* extended by cartesian product and cardinality comparison (theories *CART* and *UCART*). The quantificational case will be addressed in Section 4. Finally, in Section 5 we mention some open problems in the field of computable set theory.

2 Set-theoretic preliminaries

In this section we will briefly review some notions of set theory which will be used later.

The universe of sets we shall consider satisfies the *Zermelo-Fraenkel* axioms of set theory (see [Jec78] or [Lev79] for a complete description of the subject).

A *pairing function* $\langle \cdot, \cdot \rangle$ is any two argument function such that

$$\langle s_1, s_2 \rangle = \langle t_1, t_2 \rangle \text{ if and only if } s_1 = t_1 \wedge s_2 = t_2 ,$$

for any sets s_1, s_2, t_1, t_2.

Pairing functions can be represented in several ways. To be specific, we will adopt the Kuratowski's definition of *ordered pair*

$$\langle s_1, s_2 \rangle =_{\mathrm{Def}} \{\{s_1\}, \{s_1, s_2\}\} .$$

Given two sets s_1 and s_2, their *cartesian product* $s_1 \times s_2$ is given by

$$s_1 \times s_2 =_{\mathrm{Def}} \{\langle s_1', s_2' \rangle : s_1' \in s_1 \wedge s_2' \in s_2\} .$$

Then a *map* f (from s_1 into s_2) can be defined as any subset of $s_1 \times s_2$ such that

for all $s_1' \in s_1$ there exists a unique $s_2' \in s_2$ (denoted by $f(s_1')$) such that $\langle s_1', s_2' \rangle \in f$.

We also recall that an *ordinal* is any set s such that the following two conditions are satisfied:

(a) $(\forall u)(\forall v)((u \in s \wedge v \in s) \rightarrow (u \in v \vee u = v \vee v \in u))$, i.e. s is well ordered by the membership relation $\in$;

(b) $(\forall u)(u \in s \rightarrow u \subset s)$, i.e. s is transitive.

It is easily seen that $\emptyset$ is an ordinal; moreover, if α is an ordinal so is $\alpha \cup \{\alpha\}$, which is called the *successor* of α, otherwise written as $\alpha + 1$. This provides the von Neumann representation of natural numbers as 'finite' ordinals

$$n = \{0, 1, \ldots, n-1\} .$$

An ordinal is said to be *limit* if it is not the successor of any other ordinal. Examples of limit ordinals are $\emptyset$ and $\omega = \{0, 1, 2, \ldots, n, \ldots\}$, i.e. the set of all finite ordinals. An ordinal which is not a member of ω is *infinite*.

The *cardinality* of a set s, denoted by $|s|$, is the minimum ordinal α such that there is an injective map from s in α and viceversa. Thus, $|s_1| \leq |s_2|$ holds if there is an injection from s_1 into s_2; if in addition there is no injection from s_2 into s_1. then $|s_1| < |s_2|$.

Notice that for any two sets s_1 and s_2,

$$|s_1 \times s_2| = |s_1| \cdot |s_2| .$$

To simplify the presentation in Section 4, it will result more convenient to consider weaker notions of cartesian product and maps. Specifically, we define the *unordered* cartesian product $s_1 \otimes s_2$ of two sets s_1 and s_2 as the set of all unordered pairs of elements of s_1 and s_2, i.e.

$$s_1 \otimes s_2 =_{\mathrm{Def}} \{\{s_1', s_2'\} : s_1' \in s_1 \wedge s_2' \in s_2\} .$$

Observe that, in general,

$$|s_1 \otimes s_2| \leq |s_1| \cdot |s_2| .$$

If in addition s_1 and s_2 are disjoint, then

$$|s_1 \otimes s_2| = |s_1| \cdot |s_2| .$$

An *unordered map* h from s_1 into s_2, provided that $s_1 \cap s_2 = \emptyset$, is any subset of $s_1 \otimes s_2$ such that

for all $s_1' \in s_1$ there exists a unique $s_2' \in s_2$ (again denoted by $h(s_1')$) such that $\{s_1', s_2'\} \in h$.

Unordered maps enjoy much the same properties as ordinary maps, the main difference being that when dealing with unordered maps one has to provide explicitly a way to distinguish between the 'first' and 'second' components of their members. This, for instance, can be accomplished by specifying a set which contains the domain of the map and is disjoint from its range. Thus, if h is an unordered map with domain contained in the set s_1 (and range disjoint from s_1), then

$$h[s] =_{\mathrm{Def}} \{t' \notin s : \{s', t'\} \in h \text{ for some } s' \in s\} .$$

Finally, we recall that the *general union* of a set s is the set of all elements of elements of s, i.e., formally,

$$Un(s) =_{\mathrm{Def}} \{t : t \in u \text{ for some } u \in s\} .$$

3 The unquantified theories *CART* and *UCART*

From the unsolvability of Hilbert's tenth problem (cf. [Mat70]), it follows immediately that there is no algorithm to test whether a system of equations of the following types

$$\begin{cases} \xi = \eta \\ \xi = \eta + \zeta \\ \xi = \eta \cdot \zeta \\ \xi = k \end{cases} \tag{1}$$

(where ξ, η, and ζ stand for integer variables and k stands for an integer constant) has an integer solution or not[1]. Furthermore, for technical reasons, we can assume without loss of generality that no equation of type (1) can contain multiple occurrences of the same variable. We will refer to such equations as *simple equations*.

In this section we will show that the predicate

$$is\_solvable(\Sigma)\,,$$

which is true if and only if the system Σ of simple equations has an integer solution, can be effectively expressed in an elementary unquantified fragment of set theory (denoted *CART*), involving only the ordinary Boolean set operators, the cartesian product operator, and the cardinality comparison predicate.

More precisely, *CART* is the propositional combination of formulae of the following type

$$\begin{array}{lll} x = y \cup z\,, & x = y \cap z\,, & x = y \setminus z\,, \\ x = y \times z\,, & |x| \leq |y|\,, & |x| < |y|\,. \end{array}$$

We will provide a transformation that given a system of simple equations Σ will yield an unquantified formula φ_Σ of *CART* such that

$$is\_solvable(\Sigma) \text{ is true if and only if } \varphi_\Sigma \text{ is satisfiable}^2.$$

Thus the unsolvability of Hilbert's tenth problem will imply at once the undecidability of *CART*.

Let $\Sigma = \{\Sigma_1, \ldots, \Sigma_n\}$ be a system of simple equations $\Sigma_1, \ldots, \Sigma_n$. For each integer variable ξ in Σ we introduce n distinct set variables $x_\xi^1, \ldots, x_\xi^n$.

Let φ_0 denote the conjunction of all literals

$$x_\xi^i \cap x_\eta^j = \emptyset,$$

for all $(\xi, i) \neq (\eta, j)$, with ξ, η occurring in Σ and $1 \leq i, j \leq n$, and of all the literals

$$|x_\xi^i| = |x_\xi^j|,$$

[1] Throughout the paper, by *integer* numbers we will always mean *nonnegative* integer numbers.

[2] We recall that a set-theoretic formula φ is satisfiable if there exists an assignment of sets to the free variables of φ which makes φ true.

for all ξ occurring in Σ, $1 \leq i < j \leq n$.

For all $i = 1, \ldots, n$, we put

$$\varphi_i \equiv_{\mathrm{Def}} \begin{cases} |x^i_\xi| = |x^i_\eta| & \text{if } \Sigma_i \text{ is of type } \xi = \eta \\ |x^i_\xi| = |x^i_\eta \cup x^i_\zeta| & \text{if } \Sigma_i \text{ is of type } \xi = \eta + \zeta \\ |x^i_\xi| = |x^i_\eta \times x^i_\zeta| & \text{if } \Sigma_i \text{ is of type } \xi = \eta \cdot \zeta\ . \end{cases} \tag{2}$$

Observe that if Σ_i is of type $\xi = k$, with k an integer constant, then (2) does not define φ_i. To deal also with such equations, we need to show that the singleton operator (and therefore finite enumerations) is expressible within *CART*. This is done in the following lemma.

LEMMA 3.1 *The literal $x = \{y\}$ is expressible in CART.*

Proof. Observe that if $s_3 = s_1 \times s_2$, then $c \in s_3$ if and only if there exist $a \in s_1, b \in s_2$ such that

$$c = \{\{a\}, \{a, b\}\}.$$

Thus, $x = \{y\}$ is equisatisfiable with the following formula:

$$y \in x \wedge x \in c \wedge c \in s_1 \times s_2 \wedge b' \in c \wedge x \subseteq b' \wedge x \neq b'.$$

It is an easy matter to see that the above formula can be written using only the constructs allowed in the theory *CART*. ∎

Remark 3.1 By Lemma 3.1, finite enumerations are also expressible in *CART*, by inductively putting

$$\{x_1, \ldots, x_n\} \equiv_{\mathrm{Def}} \{x_1, \ldots, x_{n-1}\} \cup \{x_n\}.$$

□

Let K be the largest integer constant occurring in Σ, and let $v_1, \ldots, v_K$ be K distinct new variables. Then, for every simple equation Σ_i of type $\xi = k$, with k an integer constant, we put:

$$\varphi_i \equiv_{\mathrm{Def}} |x^1_\xi| = |\{v_1, \ldots, v_k\}|.$$

Also, we put

$$\varphi_{n+1} \equiv_{\mathrm{Def}} \bigwedge_{1 \leq i < j \leq K} v_i \neq v_j.$$

Notice that $\bigwedge_{i=1}^{n+1} \varphi_i$ has a set model if and only if the system Σ has a solution in the class of <u>all</u> cardinal numbers. Thus, to complete the reduction of Hilbert's tenth problem to *CART*, we only need to show that the predicate $Finite(x)$ is expressible in *CART*, where $Finite(x)$ is true if and only $|x| < \omega$. This is proved as follows.

Recall that a set s is finite if and only if it is empty or it is not equinumerous with any of its proper subsets. In particular, if s is not equinumerous with any of its proper subsets obtained by discarding just one element, it cannot be equinumerous with any other proper subset of its. On

the other hand, every infinite set is equinumerous with any of its subsets obtained by discarding one element. Thus, the predicate $Finite(x)$ is equisatisfiable with the formula

$$x = \emptyset \vee (y \in x \ \wedge \ |x \setminus \{y\}| < |x|)\,,$$

which can easily be rewritten as a formula in *CART*.

Hence, denoting by φ_{n+2} the conjunction of all literals

$$Finite(x^1_\xi)\,,$$

with ξ occurring in Σ, it follows from our construction that the predicate $is\_solvable(\Sigma)$ is equisatisfiable with the formula

$$\varphi_\Sigma \equiv_{\mathrm{Def}} \bigwedge_{i=0}^{n+2} \varphi_i. \tag{3}$$

As already observed, every conjunct in (3) can easily be written by using only constructs in *CART*. Thus, summing up, by the unsolvability of Hilbert's tenth problem, we have

THEOREM 3.1 *The unquantified theory CART has an undecidable satisfiability problem.* □

The same result also holds if in place of the ordinary cartesian product $\times$, the unordered cartesian product $\otimes$ is considered. Calling *UCART* the corresponding class of formulae, in view of the preceding discussion we only need to show that the singleton operator can be expressed in *UCART* too. We have

LEMMA 3.2 *The literal $x = \{y\}$ is expressible in UCART.*

Proof. If $s_3 = s_1 \otimes s_2$, then $c \in s_3$ if and only if there exist $a \in s_1, b \in s_2$ such that $c = \{a, b\}$. Thus the literal $x = \{y\}$ is equisatisfiable with the formula

$$y \in x \wedge x \subseteq x' \wedge x \neq x' \wedge x' \in z_1 \otimes z_2\,.$$

■

Therefore we have:

THEOREM 3.2 *The unquantified theory UCART has an undecidable satisfiability problem.* □

In the following section we will further reduce the satisfiability problem for *UCART* to the satisfiability problem for some classes of unquantified formulae of set theory.

4 The quantified case

In this section we prove the undecidability of some classes of quantified formulae of set theory.

DEFINITION 4.1 *Let $L_\in$ be the first order language with identity consisting of an unlimited supply of set variables $x_0, x_1, \ldots$; $\in$ and $=$ as only relational symbol; the propositional connectives $\wedge$, $\vee$, $\rightarrow$, $\leftrightarrow$, and $\neg$; the quantifiers $\forall$ and $\exists$. We will indicate by:*

- *Δ_0 the collection of formulae of $L_\in$ which do not contain unrestricted quantifications, i.e. all quantifiers are of type $(\forall x \in y)$ and $(\exists x \in y)$ only;*
- *$(\forall\exists\forall\cdots Q_n)_0$, where Q_n is either $\exists$ or $\forall$ according to whether n is even or odd, the collection of Δ_0-formulae which can be transformed into logically equivalent conjunctions of prenex formulae of $L_\in$ with at most $n-1$ quantifiers alternations.* □

The following are examples of $(\forall)_0$-formulae:

- $z \in x \wedge (\forall y \in x)(\forall v \in y)(v \in x)$
- $(\forall v \in x)(v \in y \vee v \in z) \wedge (\forall v \in y)(v \in x) \wedge (\forall v \in z)(v \in x)$,

whereas the following is a $(\forall\exists)_0$-formula

- $(\forall u \in x)(\exists v \in y)(u \in v) \wedge (\forall v \in y)(\forall w \in v)(w \in x)$.

Let $\mathcal{H}_1$ be the extension of the class of $(\forall)_0$-formulae with unquantified literals of type $x = y \otimes z$ and $x = Un(y)$.

Then we have the following result

THEOREM 4.1 *The theory $\mathcal{H}_1$ has an undecidable finite satisfiability problem*[3].

Proof. Since the Boolean set operator $\cup$, $\cap$, and $\setminus$ are immediately expressible by $(\forall)_0$-formulae, then, in view of Theorem 3.1, it is enough to prove that positive literals of type $|x| \leq |y|$ are also expressible in $\mathcal{H}_1$.

Recall that, by definition, $|x| \leq |y|$ holds if and only if there is an injective map from x into y. We show that under the assumption that x and y are disjoint, maps from x into y can be represented as subsets of $x \otimes y$ by using $(\forall)_0$-formulae supplemented with clauses of type $x = Un(y)$ to express the domain of such maps.

Let the predicate $is\_a\_map(f, x, y)$ stand for

$$f \subseteq x \otimes y \wedge x \subseteq Un(f) \wedge (\forall f_1' \in f)(\forall f_2' \in f)(\forall x' \in x)\left((x' \in f_1' \wedge x' \in f_2') \rightarrow f_1' = f_2'\right) .$$

It is immediate to see that if M is any set assignment satisfying the clause $is\_a\_map(f, x, y)$, and such that $Mx \cap My = \emptyset$, then the following facts hold:

[3]A set-theoretic formula φ is said to be *finitely* satisfiable if φ has a model in which every free variable is mapped into a *finite* set.

(a) Mf is a set of unordered pairs contained in $Mx \otimes My$;

(b) for each $s \in Mx$ there is a $t \in My$ such that the unordered pair $\{s,t\}$ is in Mf, i.e. the domain of Mf with respect to Mx is the whole Mx;

(c) if $\{s,t\}, \{s,t'\} \in Mf$, with $s \in Mx$, then $t = t'$, i.e. Mf is singlevalued.

Thus, $x \cap y = \emptyset \wedge \mathit{is\_a\_map}(f,x,y)$ expresses that f is an unordered map from x into y (see Section 2). Also, if we denote by $\mathit{injective}(f,x,y)$ the formula

$$\mathit{is\_a\_map}(f,x,y) \wedge (\forall f_1' \in f)(\forall f_2' \in f)(\forall y' \in y)\left((y' \in f_1' \wedge y' \in f_2') \rightarrow f_1' = f_2'\right) ,$$

it is plain that $x \cap y = \emptyset \wedge \mathit{injective}(f,x,y)$ expresses that f is an injective unordered map from x into y. Thus, $x \cap y = \emptyset \wedge \mathit{injective}(f,x,y)$ is equisatisfiable with $x \cap y = \emptyset \wedge |x| \leq |y|$.

To get rid of the extra-assumption $x \cap y = \emptyset$, one can introduce new variables x_1 and y_1 which stand for disjoint sets having the same cardinality of x and y respectively. Thus, $|x| \leq |y|$ is equisatisfiable with

$$\begin{array}{l} x \cap x_1 = \emptyset \wedge y \cap y_1 = \emptyset \wedge x_1 \cap y_1 = \emptyset \\ \quad \wedge \mathit{injective}(f_1, x, x_1) \wedge \mathit{injective}(f_2, x_1, x) \wedge \mathit{injective}(f_3, y, y_1) \\ \quad \wedge \mathit{injective}(f_4, y_1, y) \wedge \mathit{injective}(f_5, x_1, y_1) . \end{array}$$

Observe that all constructs of $CART$ with the only exception of the predicate $|x| < |y|$ have been expressed with formulae of the theory $\mathcal{H}_1$. In the undecidability results of the preceding section, the predicate $|x| < |y|$ has been used only to show that the predicate $\mathit{Finite}(x)$ was expressible. It appears that to express $|x| < |y|$ a quantifier alternation is needed. Therefore at this stage we can only conclude that the finite satisfiability problem for $\mathcal{H}_1$ is unsolvable. ■

As immediate corollaries we obtain:

COROLLARY 4.1 *The extension $\mathcal{H}_2$ of the theory $\mathcal{H}_1$ with unquantified clauses of type $\mathit{Finite}(x)$ has an unsolvable satisfiability problem.* □

COROLLARY 4.2 *The extension $\mathcal{H}_3$ of the theory $\mathcal{H}_1$ with unquantified literals of type $x \in \omega$, where ω denotes the first infinite limit ordinal, has an unsolvable satisfiability problem.*

Proof. It is enough to observe that $\mathit{Finite}(x)$ is equisatisfiable with $y \in \omega \wedge |x| = |y|$. ■

Next we show that all constructs of the theory $\mathcal{H}_3$ are expressible by $(\forall\exists)_0$-formulae, therefore proving the undecidability of this latter theory. Obviously, we only need to show that all literals of type $x = \mathit{Un}(x)$, $x = y \otimes z$, and the constant ω are expressible by $(\forall\exists)_0$-formulae.

Literals of type $x = \mathit{Un}(y)$:

By definition, $x = \mathit{Un}(y)$ is logically equivalent to the $(\forall\exists)_0$-formula

$$(\forall x' \in x)(\exists y' \in y)(x' \in y') \wedge (\forall y' \in y)(\forall y'' \in y')(y'' \in x) .$$

Literals of type $x = y \otimes z$:

Consider the formulae

$$
\begin{aligned}
\mathcal{A} &\equiv_{\mathrm{Def}} (\forall x' \in x)(\forall x''_1 \in x')(\forall x''_2 \in x')(\forall x''_3 \in x')(x''_1 = x''_2 \vee x''_1 = x''_3 \vee x''_2 = x''_3) \\
\mathcal{B} &\equiv_{\mathrm{Def}} Un(x) \subseteq y \cup z \\
\mathcal{C} &\equiv_{\mathrm{Def}} (\forall y' \in y)(\forall z' \in z)(\exists x' \in x)(y' \in x' \wedge z' \in z) .
\end{aligned}
$$

Plainly, $\mathcal{A}$ says that x is a set of unordered pairs, $\mathcal{B}$ says that the elements of each unordered pair in x belong to $y \cup z$, and $\mathcal{C}$ says that any unordered pair of $y \otimes z$ is contained in some element of x. Thus $\mathcal{A} \wedge \mathcal{B} \wedge \mathcal{C}$ is equisatisfiable with $x = y \otimes z$.

Notice that at this point from Corollary 4.1 we have

LEMMA 4.1 *The class of $(\forall\exists)_0$-formulae has an unsolvable finite satisfiability problem.* □

The constant ω:

Let *is_an_ordinal*(z) stand for the $(\forall\exists)_0$-formula

$$(\forall z'_1 \in z)(\forall z'_2 \in z)(z'_1 = z'_2 \vee z'_1 \in z'_2 \vee z'_2 \in z'_1) \wedge (\forall z' \in z)(\forall z'' \in z')(z'' \in z) . \tag{4}$$

Also, denote by *infinite_limit_ordinal*(z) the formula

$$is\_an\_ordinal(z) \wedge \emptyset \in z \wedge (\forall z'_1 \in z)(\exists z'_2 \in z)(z'_1 \in z'_2) . \tag{5}$$

Plainly, if M satisfies *infinite_limit_ordinal*(z), then Mz must indeed be an infinite limit ordinal. In fact, from the first conjunt of (4), Mz is well-ordered by $\in$. In addition, the second conjunct of (4) forces Mz to be transitive. Thus, Mz is an ordinal. Finally, the last two conjuncts of (5) imply that Mz is an infinite limit ordinal.

In addition, notice that the predicate $y = f[x]$, i.e. y is the image under f of the set x, where f is an unordered map, is expressed by the following formula:

$$
\begin{aligned}
&(\forall y' \in y)(\exists f' \in f)(\exists x' \in x)(y' \in f' \wedge x' \in f') \\
&\quad \wedge(\forall f' \in f)(\forall y' \in f')(\forall x' \in x)\left((x' \neq y' \wedge x' \in f') \rightarrow y' \in y\right) .
\end{aligned}
$$

We claim that the following $(\forall\exists)_0$-formula characterizes the constant ω.

$$
\begin{aligned}
&infinite\_limit\_ordinal(z) \wedge z_1 \cup z_2 = z \wedge z_1 \cap z_2 = \emptyset \\
&\quad \wedge is\_a\_map(f, z_1, z_2) \wedge is\_a\_map(g, z_2, z_1) \\
&\quad \wedge(\forall z'_1 \in z_1)(\exists f' \in f)(\exists f'' \in f')(f'' \in z_2 \wedge z'_1 \in f'' \wedge z'_1 \in f') \\
&\quad \wedge(\forall z'_2 \in z_2)(\exists g' \in g)(\exists g'' \in g')(g'' \in z_1 \wedge z'_2 \in g'' \wedge z'_2 \in g') \\
&\quad \wedge f[z_1] = z_2 \setminus \{\emptyset\} \wedge g[z_2] = z_1 \setminus \{\emptyset\}
\end{aligned} \tag{6}
$$

Notice that by using the usual notation of point map evaluation, the sixth and seventh conjuncts of the above formula could have been rewritten respectively as

$$(\forall z'_1 \in z_1)(z'_1 \in f(z'_1))$$

and

$$(\forall z_2' \in z_2)(z_2' \in g(z_2'))\ .$$

We have to prove that

I. (6) is satisfiable, and

II. $Mz = \omega$, in any model M of (6).

Concerning *I*, it is an easy matter to verify that the following assignment M satisfies (6).

$$\begin{aligned} Mz &= \omega \\ Mz_1 &= \{2n : n \in \omega\} \quad (= \omega_{\text{even}}) \\ Mz_2 &= \{2n+1 : n \in \omega\} \quad (= \omega_{\text{odd}}) \\ Mf &= \{\{2n, 2n+1\} : n \in \omega\} \\ Mg &= \{\{2n-1, 2n\} : n \in \omega \setminus \{0\}\}\ . \end{aligned}$$

Next we prove *II*. So, let M be a model of (6). Let $\zeta = Mz$, $Z_1 = Mz_1$, $Z_2 = Mz_2$, $F_0 = Mf$, $F_1 = Mg$. Since $0 \in \zeta = Z_1 \cup Z_2$, we can assume without loss of generality that $0 \in Z_1$. Then we claim that

$$\omega_{\text{even}} \subseteq Z_0\ , \quad \omega_{\text{odd}} \subseteq Z_1 \tag{7}$$

and, for all $n \in \omega$,

$$F_0(2n) = 2n+1 \qquad \text{and} \qquad F_1(2n+1) = 2n+2\ . \tag{8}$$

We will prove (7) and (8) by induction on n.

Let $p(j)$ be the parity function defined by

$$p(j) = \begin{cases} 0 & \text{if } j \text{ is even} \\ 1 & \text{if } j \text{ is odd}\ . \end{cases}$$

Assume that $j \in Z_{p(j)}$, for all $j < n$, and that, additionally, if $j+1 < n$ then $F_{p(j)}(j) = j+1$. Then we need to show that $n \in Z_{p(n)}$ and $F_{p(n-1)}(n-1) = n$. Since by (6) $n \in F_0[Z_0] \cup F_1[Z_1]$, then $F_{i_0}(j_0) = n$, for some $i_0 \in \{0,1\}$, $j_0 \in \{0,1,\ldots,n-1\}$. Observe that $j_0 = n-1$, for otherwise $F_{p(j_0)}(j_0) = j_0 + 1 < n$. Thus, $i_0 = p(n-1)$ and $F_{p(n-1)}(n-1) = n$, so that we have also $n \in Z_{1-p(n-1)} = Z_{p(n)}$.

From (7) and (8), it follows that $Mz = \omega$. Indeed, if $Mz = \zeta > \omega$, then $\omega \in \zeta = Z_0 \cup Z_1$, and hence $F_{i_0}(j_0) = \omega$, for some $i_0 \in \{0,1\}$ and $j_0 \in \omega$. But this is a contradiction, since, by (8), $F_{i_0}(j_0) = j_0 + 1$. This proves that $Mz = \omega$.

From Corollary 4.2, it then follows

THEOREM 4.2 *The class of* $(\forall\exists)_0$*-formulae is undecidable.* □

5 Open problems

In the previous section we showed that the satisfiability problem for the class $(\forall\exists)_0$ is undecidable. To settle down the decidability question for the entire hierarchy Δ_0 (see Definition 4.1), the main problem which remains to investigate is the satisfiability problem for the $(\forall)_0$-formulae. As we mentioned in the introductory section, we conjecture that such a class is decidable. Evidence for this is that in the absence of the axiom of foundation, the $(\forall)_0$-formulae can be decided by the same procedure given in [BFOS81] for the subclass of simple prenex formulae.

At any rate, notice that:

- a positive answer to this question will stress the need to investigate the decidability problem for all the intermediate classes of formulae as, for instance, the theory $\mathcal{H}_1$ (cf. previous section);
- on the other hand, a negative answer, will bring to attention all the unquantified theories, which have not been investigated yet, as for instance,
  - MLS extended by the cartesian product,
  - MLS extended by the powerset and the general union operators.

References

[BFOS81] M. Breban, A. Ferro, E.G. Omodeo, and J.T. Schwartz. Decision procedures for elementary sublanguages of set theory. II. Formulas involving restricted quantifiers, together with ordinal, integer, map, and domain notions. *Comm. Pure App. Math.*, XXXIV:177–195, 1981.

[Can] D. Cantone. Decision procedures for elementary sublanguages of set theory. X. Multilevel syllogistic extended by the singleton and powerset operators. *Journal of Symbolic Computation - Special issue on New trends in Automated Mathematical Reasoning - Proceedings.* To appear.

[CC88a] D. Cantone and V. Cutello. Decision procedures for elementary sublanguages of set theory. XV. Multilevel syllogistic extended by the predicate *finite* and the operators singleton and $pred_<$. *Rapporto di ricerca del Dipartimento di Matematica ed Informatica della Universita' di Udine n. 39*, 1988. To appear in *J. Automated Reasoning.*

[CC88b] D. Cantone and V. Cutello. *Some decidability results on quantified sublanguages of set theory.* Technical Report 378, New York University, Comp. Sci. Dept., 1988.

[CC89] D. Cantone and V. Cutello. *A decision procedure for set-theoretic formulae involving rank and cardinality comparison.* Technical Report 440, Comp. Sci. Dept. New York University, 1989. Submitted to *3rd Italian Conference on Theoretical Computer Science, Mantova, November 2-4, 1989.*

[CCF88] D. Cantone, V. Cutello, and A. Ferro. Decision procedures for elementary sublanguages of set theory. XIV. Three languages involving rank related constructs. In *International Symposium on Symbolic and Algebraic Computation*, 1988. To appear in the series *Lecture Notes in Computer Science*, Springer-Verlag.

[CFMS87] D. Cantone, A. Ferro, B. Micale, and G. Sorace. Decision procedures for elementary sublanguages of set theory. IV. Formulae involving a rank operator or one occurrence of $\Sigma(x) = \{\{y\}|y \in x\}$. *Comm. Pure App. Math.*, XL:37–77, 1987.

[CFO] D. Cantone, A. Ferro, and E.G. Omodeo. *Computable Set Theory.* Oxford University Press, to appear.

[CFO88] D. Cantone, A. Ferro, and E.G. Omodeo. Decision procedures for elementary sublanguages of set theory. VIII. A semidecision procedure for finite satisfiability of unquantified set-theoretic formulae. *Comm. Pure App. Math.*, XLI:105–120, 1988.

[CFOP88] D. Cantone, A. Ferro, E.G. Omodeo, and A. Policriti. *Sillogistica con operatore di scelta.* Technical Report 34, University of Udine, 1988.

[CFS85] D. Cantone, A. Ferro, and J.T. Schwartz. Decision procedures for elementary sublanguages of set theory. VI. Multi-level syllogistic extended by the powerset operator. *Comm. Pure App. Math.*, XXXVIII:549–571, 1985. Special anniversary issue.

[CFS87] D. Cantone, A. Ferro, and J.T. Schwartz. Decision procedures for elementary sublanguages of set theory. V. Multi-level syllogistic extended by the general union operator. *Journal of Computer and System Sciences*, 34(1):1–18, 1987.

[CS88] D. Cantone and J.T. Schwartz. A set-theoretically based proof verifier. 1988. Manuscript.

[CS] D. Cantone and J.T. Schwartz. Decision procedures for elementary sublanguages of set theory. XI. Multilevel syllogistic extended by some elementary map constructs. *Journal of Symbolic Computation - Special issue on New trends in Automated Mathematical Reasoning - Proceedings.* To appear.

[Dav73] M. Davis. Hilbert's tenth problem is unsolvable. *American Mathematical Monthly*, 80:233–269, 1973.

[DMR76] M. Davis, Y. Matijasevič, and J. Robinson. Hilbert's tenth problem. Diophantine equations: positive aspects of a negative solution. In *Proceedings of Symposia in Pure Mathematics*, pages 323–378, 1976.

[Fer] A. Ferro. Decision procedures for elementary sublanguages of set theory. XII. Multilevel syllogistic extended with singleton and choice operators. *Journal of Symbolic Computation - Special issue on New trends in Automated Mathematical Reasoning - Proceedings.* To appear.

[FO87] A. Ferro and E.G. Omodeo. Decision procedures for elementary sublanguages of set theory. VII. Validity in set theory when a choice operator is present. *Comm. Pure App. Math.*, XL:265–280, 1987.

[FOS80a] A. Ferro, E.G. Omodeo, and J.T. Schwartz. Decision procedures for elementary sublanguages of set theory. I. Multi-level syllogistic and some extensions. *Comm. Pure App. Math.*, XXXIII:599–608, 1980.

[FOS80b] A. Ferro, E.G. Omodeo, and J.T. Schwartz. *Decision procedures for some fragments of Set Theory.* Volume 87 of *Lecture Notes in Computer Science*, Springer-Verlag, 1980.

[Gog78] D. Gogol. The $\forall_n\exists$-completeness of Zermelo-Fraenkel set theory. *Zeitschr. f. math. Logik und Grundlagen d. Math.*, 1978.

[Gog79] D. Gogol. Sentences with three quantifiers are decidable in set theory. *Fundamenta Mathematicae*, CII, 1979.

[Jec78] T.J. Jech. *Set theory.* Academic Press, New York, 1978.

[Lev79] A. Levy. *Basic Set Theory.* Springer-Verlag, 1979.

[Mat70] Y. Matijasevič. Enumerable sets are Diophantine sets. *Soviet Math. Doklady*, 11:354–357, 1970.

[PP88] F. Parlamento and A. Policriti. Decision procedures for elementary sublanguages of set theory. IX. Unsolvability of the decision problem for a restricted subclass of the Δ_0-formulas in set theory. *Comm. Pure App. Math.*, XLI:221–251, 1988.

[PP] F. Parlamento and A. Policriti. Decision procedures for elementary sublanguages of set theory. XIII. Model graphs, reflection and decidability. *Journal of Symbolic Computation - Special issue on New trends in Automated Mathematical Reasoning - Proceedings.* To appear.

NYU COMPSCI TR-449
Cantone, D
Set-theoretic reductions of
Hilbert's tenth problem.
c.2